Eksploitasi Tool: CyberSufi PowerShell 7

Sebenarnya bagian ini secara prinsip sama saja dengan pembuatan tool sebelumnya (CyberSufi PowerMenu 7).

Perbedaan yang mendasar adalah kita membuat suatu menu sederhana yang menampung perintah-perintah langsung via **Shell**... tidak dari perintah **Rundll32**.

Kita tetap akan membuat suatu ikon *hardwired* dan memasangkan perintah-perintah tersebut padanya. Pengaktifan menu perintah dilakukan dengan klik kanan.

Dan kita juga akan membuatnya ke dalam file REG.

Oleh karena mirip, maka saya akan jelaskan secara cepat, ya?

5.1 Membuat Program Penginstal

Berikut ini kita akan membuat program berbasis REG, untuk mewujudkan angan-angan kita. Caranya sebagai berikut.

5.1.1 Langkah 1: Memasangkan Pengaktifan CLSID pada Desktop

Perintah pemasangan CLSID ini dilakukan dengan perintah:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ex
plorer\Desktop\NameSpace\{a1234567-1234-1234-1234-123456789abe}]
```

Perintah tersebut berarti kita membentuk subkey baru dengan nama {a1234567-1234-1234-1234-123456789abe}, pada subkey NameSpace.

5.1.2 Langkah 2: Membentuk clsid Utama

Pada tool CSPS7, CLSID yang akan kita bentuk adalah:

a1234567-1234-1234-1234-123456789abe

Pembentukan CLSID utama ini, bila kita tuangkan dalam suatu format file REG, maka akan terlihat seperti listing program berikut ini.

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-123456789abe}]
@="CyberSufi PowerShell 7"
```

Keterangan:

- `[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-123456789abe}]`

Baris ini menunjukkan bahwa kita membuat suatu CLSID, pada subkey CLSID yang berada di dalam key HKEY_CLASSES_ROOT.

- `@="CyberSufi PowerShell 7"`

Tanda **@ m**enunjukkan nilai ***default*** untuk subkey {a1234567-1234-1234-1234-123456789abe}. Sedangkan isi datanya adalah **CyberSufi PowerShell 7** dengan jenis data string.

5.1.3 Langkah 3: Membuat Subkey untuk Gambar Ikon

Untuk dapat mengaktifkan menu, maka dibutuhkan suatu ikon yang akan kita pasangkan pada desktop. Gambar atau bentuk dari ikon tersebut kita buat dengan perintah berikut.

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\DefaultIcon]
@="shell32.dll,13"
```

Keterangan:

- `[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-123456789abe}\DefaultIcon]`

Membentuk suatu subkey baru yang bernama **DefaultIcon** pada subkey {a1234567-1234-1234-1234-123456789abe}.

- `@="shell32.dll,13"`

Memasangkan nilai default untuk gambar ikon yang kita ambil dari file milik Windows yang bernama shell32.dll. Sedangkan ikon yang dipakai adalah nomor 13.

5.1.4 Langkah 4: Membuat Subkey untuk Menu Utama

Subkey utama yang digunakan untuk menampung data-data ada pada subkey **Shell**. Perintah yang kita tuliskan adalah sebagai berikut.

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell]
@=""
```

Keterangan:

- `[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-123456789abe}\Shell]`

Membentuk subkey yang bernama **Shell** dan diletakkan di bawah subkey {a1234567-1234-1234-1234-123456789abe}.

- `@=""`

Subkey **Shell** nilai defaultnya tidak kita biarkan kosong.

5.1.5 Langkah 5: Membuat Subkey untuk Menu Tambahan

Untuk menambah kelancaran program, kita bentuk menu tambahan. Nama subkey tersebut adalah **ShellFolder** sebagai berikut.

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\ShellFolder]
"Attributes"=hex:00,00,00,00
```

Keterangan:

- `[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-123456789abe}\ShellFolder]`

Membentuk subkey yang bernama ShellFolder dan diletakkan di bawah subkey {a1234567-1234-1234-1234-123456789abe}.

- `"Attributes"=hex:00,00,00,00`

Data yang ada pada subkey tersebut adalah **Attributes**. Isi data ini adalah 0 (nol) dan kita masukkan dengan jenis data Binary.

5.1.6 Langkah 6: Membuat Isian yang Membentuk Menu

Pada bagian inilah sebetulnya kita menempatkan perintah-perintah yang membuat program bekerja.

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ Administrative Tools]
```

Keterangan:

- `[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-123456789abe}\Shell\ Administrative Tools]`

Membentuk subkey yang bernama **Administrative Tools** dan diletakkan di bawah subkey **Shell**.

- `[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-123456789abe}\Shell\ Administrative Tools\Command]`
- `@="Explorer.exe shell:Administrative Tools"`

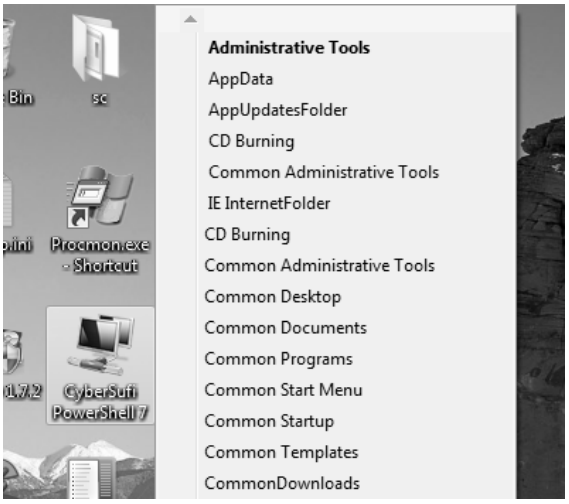
Membentuk subkey yang bernama **Command** dan diletakkan di bawah subkey **Administrative Tools**. Datanya adalah **default** alias **@**. Pada data default (@) kita isi dengan data perintah pengaktifan. Untuk dapat memasukkan perintahnya, kita dapat melihat dari pembahasan Eksploitasi Shell.

Anggap saja, kita telah memasukkan semua data perintah yang ada ke dalam file REG. Kita aktifkan (merge/gabung) program dengan mengklik ganda file tersebut. Jika setingan Windows Anda masih standar, maka akan keluarlah UAC Windows, yang meminta izin pengaktifan program Regedit. Jawab saja **Yes**. Akan keluar pesan konfirmasi dari program Registry Editor. Jawab saja **Yes**. Maka keluarlah pesan sukses dari Windows.

Jika kita tengok desktop suatu *hardwired icon* dengan judul: *CyberSufi PowerShell 7* akan muncul.

Gambar 5.1 Ikon program CSPS7

Seandainya kita klik kanan ikon *hardwired* tersebut, menu konteks akan muncul, berisi perintah yang kita ketikkan.



Gambar 5.2 Klik kanan menampilkan menu program

5.1.7 Listing Program CSPS7

Berikut ini listing program untuk menginstal program PowerShell. Silakan dipelajari (sendiri … ☺).

```
Windows Registry Editor Version 5.00

;------------------------------------------------------------
;CyberSufi Power Shell for Windows 7 - Installation Program
;(C)CopyLeft, 2010 - Tri Amperiyanto
;email : megatruh@hotmail.com, megatruh@ymail.com
;web : www.cybersufi-online.co.cc
;------------------------------------------------------------
;---pasang icon di desktop
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
explorer\Desktop\NameSpace\{a1234567-1234-1234-1234-
123456789abe}]

;---buat clsid utama
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}]
@="CyberSufi PowerShell 7"
```

```
;---buat subkey untuk gambar icon
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\DefaultIcon]
@="shell32.dll,13"

;buat subkey untuk menu utama
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell]
@=""

;buat subkey untuk menu tambahan
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\ShellFolder]
"Attributes"=hex:00,00,00,00

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ Administrative Tools]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ Administrative Tools\Command]
@="Explorer.exe shell:Administrative Tools"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ AppData]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ AppData\Command]
@="Explorer.exe shell:AppData"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ AppUpdatesFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ AppUpdatesFolder\Command]
@="Explorer.exe shell:AppUpdatesFolder "

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ CD Burning]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CD Burning\Command]
@="Explorer.exe shell:CD Burning"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Administrative Tools]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Administrative Tools\Command]
@="Explorer.exe shell:Common Administrative Tools"


;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Desktop]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Desktop\Command]
@="Explorer.exe shell:Common Desktop"
```

```
;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Documents]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Documents\Command]
@="Explorer.exe shell:Common Documents"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Programs]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Programs\Command]
@="Explorer.exe shell:Common Programs"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Start Menu]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Start Menu\Command]
@="Explorer.exe shell:Common Start Menu"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Startup]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Startup\Command]
@="Explorer.exe shell:Common Startup"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Templates]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Common Templates\Command]
@="Explorer.exe shell:Common Templates"


;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonDownloads]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonDownloads\Command]
@="Explorer.exe shell:CommonDownloads"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonMusic]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonMusic\Command]
@="Explorer.exe shell:CommonMusic "

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonPictures]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonPictures\Command]
@="Explorer.exe shell:CommonPictures"
```

```
;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonRingtones]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonRingtones\Command]
@="Explorer.exe shell:CommonRingtones"


;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonVideo]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CommonVideo\Command]
@="Explorer.exe shell:CommonVideo"


;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ConflictFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ConflictFolder\Command]
@="Explorer.exe shell:ConflictFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ConnectionsFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ConnectionsFolder\Command]
@="Explorer.exe shell:ConnectionsFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Contacts]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Contacts\Command]
@="Explorer.exe shell:Contacts"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ControlPanelFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ControlPanelFolder\Command]
@="Explorer.exe shell:ControlPanelFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Cookies]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Cookies\Command]
@="Explorer.exe shell:Cookies"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CredentialManager]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CredentialManager\Command]
@="Explorer.exe shell:CredentialManager"
```

```
;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CryptoKeys]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\CryptoKeys\Command]
@="Explorer.exe shell:CryptoKeys"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Default Gadgets]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Default Gadgets\Command]
@="Explorer.exe shell:Default Gadgets"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Desktop]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Desktop\Command]
@="Explorer.exe shell:Desktop"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Device Metadata Store]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Device Metadata Store\Command]
@="Explorer.exe shell:Device Metadata Store"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\DocumentsLibrary]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\DocumentsLibrary\Command]
@="Explorer.exe shell:DocumentsLibrary"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Downloads]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Downloads\Command]
@="Explorer.exe shell:Downloads"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\DpapiKeys]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\DpapiKeys\Command]
@="Explorer.exe shell:DpapiKeys"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Favorites]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Favorites\Command]
@="Explorer.exe shell:Favorites"

;-------------------------
```

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Fonts]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Fonts\Command]
@="Explorer.exe shell:Fonts"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Gadgets]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Gadgets\Command]
@="Explorer.exe shell:Gadgets"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Games]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Games\Command]
@="Explorer.exe shell:Games "

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\GameTasks]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\GameTasks\Command]
@="Explorer.exe shell:GameTasks"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\History]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\History\Command]
@="Explorer.exe shell:History"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ImplicitAppShortcuts]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ImplicitAppShortcuts\Command]
@="Explorer.exe shell:ImplicitAppShortcuts"


;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ IE InternetFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ IE InternetFolder\Command]
@="Explorer.exe shell:InternetFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Libraries]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Libraries\Command]
@="Explorer.exe shell:Libraries"

;-------------------------
```

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Links]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Links\Command]
@="Explorer.exe shell: Links "

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Local AppData]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Local AppData\Command]
@="Explorer.exe shell:Local AppData"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\LocalizedResourcesDir]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\LocalizedResourcesDir\Command]
@="Explorer.exe shell:LocalizedResourcesDir"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\MAPIFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\MAPIFolder\Command]
@="Explorer.exe shell:MAPIFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\MusicLibrary]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\MusicLibrary\Command]
@="Explorer.exe shell:MusicLibrary"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\My Music]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\My Music\Command]
@="Explorer.exe shell:My Music"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\My Pictures]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\My Pictures\Command]
@="Explorer.exe shell:My Pictures"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\My Video]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\My Video\Command]
@="Explorer.exe shell:My Video"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\MyComputerFolder]
```

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\MyComputerFolder\Command]
@="Explorer.exe shell:MyComputerFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\NetHood]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\NetHood\Command]
@="Explorer.exe shell:NetHood"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\NetworkPlacesFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\NetworkPlacesFolder\Command]
@="Explorer.exe shell:NetworkPlacesFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\OEM Links]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\OEM Links\Command]
@="Explorer.exe shell:OEM Links"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Original Images]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Original Images\Command]
@="Explorer.exe shell:Original Images"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\OtherUsersFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\OtherUsersFolder\Command]
@="Explorer.exe shell:OtherUsersFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Personal]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Personal\Command]
@="Explorer.exe shell:Personal"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PhotoAlbums]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PhotoAlbums\Command]
@="Explorer.exe shell:PhotoAlbums"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PicturesLibrary]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PicturesLibrary\Command]
```

```
@="Explorer.exe shell:PicturesLibrary"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Playlists]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Playlists\Command]
@="Explorer.exe shell:Playlists"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PrintersFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PrintersFolder\Command]
@="Explorer.exe shell:PrintersFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PrintHood]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PrintHood\Command]
@="Explorer.exe shell:PrintHood"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Profile]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Profile\Command]
@="Explorer.exe shell:Profile"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFiles]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFiles\Command]
@="Explorer.exe shell:ProgramFiles"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFilesCommon]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFilesCommon\Command]
@="Explorer.exe shell:ProgramFilesCommon"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFilesCommonX86]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFilesCommonX86\Command]
@="Explorer.exe shell:ProgramFilesCommonX86"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFilesX86]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ProgramFilesX86\Command]
@="Explorer.exe shell:ProgramFilesX86"
```

```
;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Programs]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Programs\Command]
@="Explorer.exe shell:Programs"


;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Public]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Public\Command]
@="Explorer.exe shell:Public"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PublicGameTasks]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PublicGameTasks\Command]
@="Explorer.exe shell:PublicGameTasks"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PublicSuggestedLocations]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\PublicSuggestedLocations\Command]
@="Explorer.exe shell:PublicSuggestedLocations"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Quick Launch]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Quick Launch\Command]
@="Explorer.exe shell:Quick Launch"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Recent]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Recent\Command]
@="Explorer.exe shell:Recent"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\RecycleBinFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\RecycleBinFolder\Command]
@="Explorer.exe shell:RecycleBinFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ResourceDir]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\ResourceDir\Command]
@="Explorer.exe shell:ResourceDir"

;-------------------------
```

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Ringtones]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Ringtones\Command]
@="Explorer.exe shell:Ringtones"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SampleMusic]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SampleMusic\Command]
@="Explorer.exe shell:SampleMusic"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SamplePictures]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SamplePictures\Command]
@="Explorer.exe shell:SamplePictures"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SamplePlaylists]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SamplePlaylists\Command]
@="Explorer.exe shell:SamplePlaylists"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SampleVideos]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SampleVideos\Command]
@="Explorer.exe shell:SampleVideos"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SavedGames]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SavedGames\Command]
@="Explorer.exe shell:SavedGames"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Searches]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Searches\Command]
@="Explorer.exe shell:Searches"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SearchHomeFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SearchHomeFolder\Command]
@="Explorer.exe shell:SearchHomeFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SendTo]
```

```
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SendTo\Command]
@="Explorer.exe shell:SendTo"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Start Menu]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Start Menu\Command]
@="Explorer.exe shell:Start Menu"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Startup]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Startup\Command]
@="Explorer.exe shell:Startup"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SyncCenterFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SyncCenterFolder\Command]
@="Explorer.exe shell:SyncCenterFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SyncResultsFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SyncResultsFolder\Command]
@="Explorer.exe shell:SyncResultsFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SyncSetupFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SyncSetupFolder\Command]
@="Explorer.exe shell:SyncSetupFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\System]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\System\Command]
@="Explorer.exe shell:System"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SystemCertificates]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SystemCertificates\Command]
@="Explorer.exe shell:SystemCertificates"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SystemX86]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\SystemX86\Command]
```

```
@="Explorer.exe shell:SystemX86"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Templates]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Templates\Command]
@="Explorer.exe shell:Templates"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\TreePropertiesFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\TreePropertiesFolder\Command]
@="Explorer.exe shell:TreePropertiesFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\User Pinned]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\User Pinned\Command]
@="Explorer.exe shell:User Pinned"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\UserProfiles]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\UserProfiles\Command]
@="Explorer.exe shell:UserProfiles"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\UsersFilesFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\UsersFilesFolder\Command]
@="Explorer.exe shell:UsersFilesFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\UsersLibrariesFolder]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\UsersLibrariesFolder\Command]
@="Explorer.exe shell:UsersLibrariesFolder"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\VideosLibrary]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\VideosLibrary\Command]
@="Explorer.exe shell:VideosLibrary"

;-------------------------
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Windows]
[HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}\Shell\Windows\Command]
@="Explorer.exe shell:Windows"
```

5.2 Membuat Program Uninstall

Program ini digunakan untuk melakukan uninstall program PowerShell7. Saya tidak akan berpanjang lebar. Teliti sendiri ya? Lihat pembahasan di depan.

5.2.1 Listing Program UNCSPS7

```
Windows Registry Editor Version 5.00

;------------------------------------------------------------
;CyberSufi Power Shell for Windows 7  - Uninstall Program
;(C)CopyLeft, 2010 - Tri Amperiyanto
;email : megatruh@hotmail.com, megatruh@ymail.com
;web : www.cybersufi-online.co.cc
;------------------------------------------------------------
[-HKEY_CLASSES_ROOT\CLSID\{a1234567-1234-1234-1234-
123456789abe}]
[-KEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
explorer\Desktop\NameSpace\{a1234567-1234-1234-1234-
123456789abe}]
```

Oke! Selesai sudah tools eksploitasi kedua kita.

***